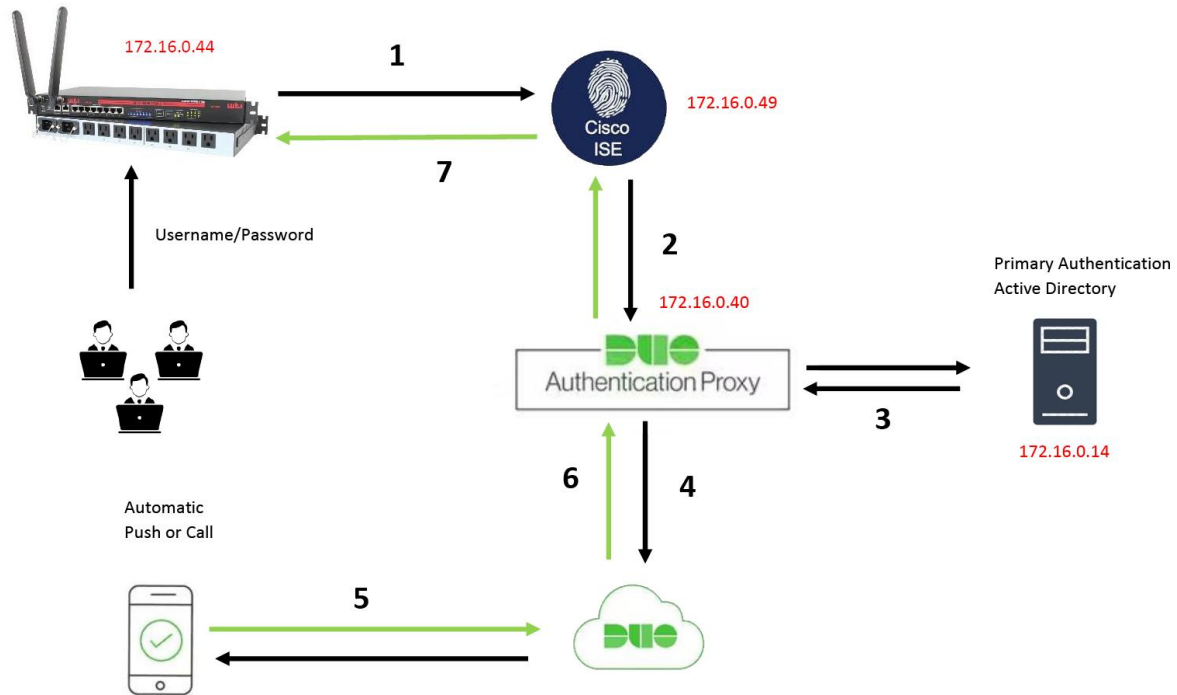


DUO with Active Directory and Cisco ISE NAS-Identifier with WTI Radius client



Introduction

This document describes how to configure Duo push integration with Active Directory (AD) and Cisco Identity Service (ISE) as Two-Factor Authentication that connect to WTI Radius client.

Components used

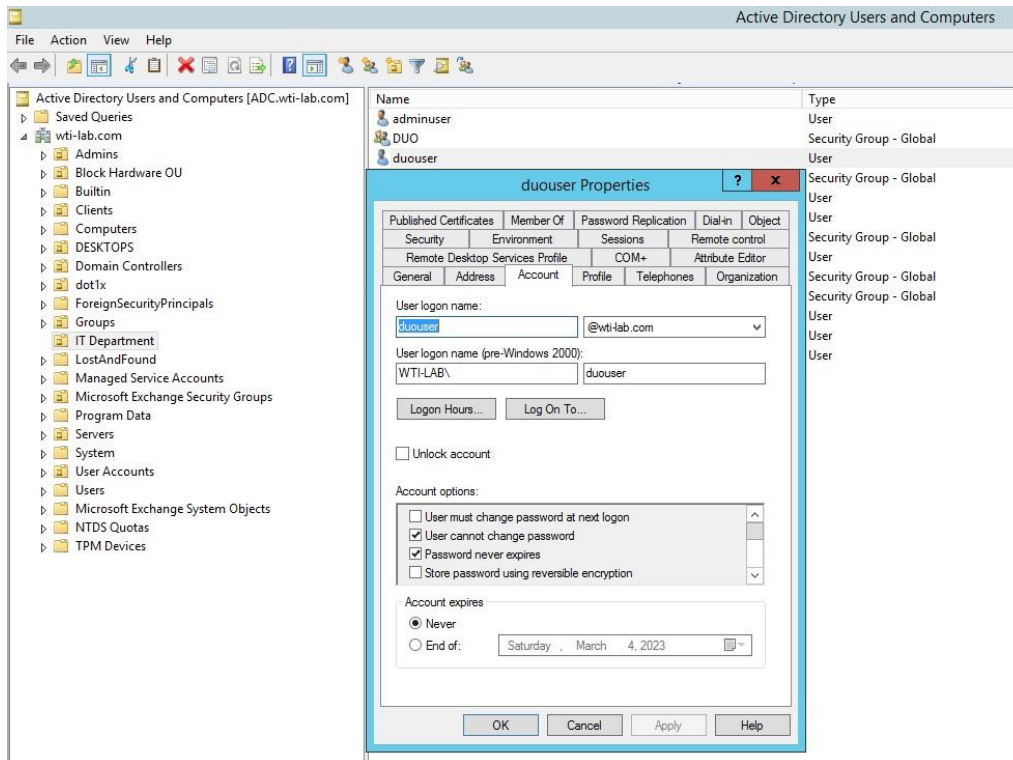
- Windows Active Directory
- Duo
- Duo Authentication Proxy Manager
- Cisco ISE
- WTI Radius client

Communication process

1. WTI makes an authentication request to Cisco ISE
2. Cisco ISE sends authentication request to the Duo Authentication Proxy
3. Duo Proxy sends a request to Active Directory
4. Duo Authentication Proxy connection established to Duo security over TCP port 443
5. Secondary authentication via Duo Security's service
6. Duo authentication proxy receives authentication response
7. Cisco ISE return to WTI with Access Accept + Radius attribute 41 and WTI permits the user access.

Active Directory Configurations

1. Navigate to Active Directory Users and Computers > Add new User and Password. In this example we created **duouser** account in active directory users and computers.



Duo configuration

1. Log in into your Duo Admin portal
2. On the left side panel, navigate to **Users**, click **Add User** and type the name of the user that matches your Active Domain username, then click Add User.

Dashboard

Policies

Applications

Users

Add User

Pending Enrollments

Bulk Enroll Users

Import Users

Directory Sync

Bypass Codes

Groups

2FA Devices

Search for users, groups, applications, or devices

Dashboard > Users > Add User

Add User

Most applications allow users to enroll themselves after they complete primary authentication. [Learn more about adding users](#)

Username:

Should match the primary authentication username.

Add User

3. On the new user's panel, fill in the blank all the necessary information.

4. Under user devices specify the secondary authentication method. Click **Add Phone**

Phones

You may rearrange the phones by dragging and dropping in the table. [Learn more about activating a replacement phone](#)

This user has no phones. [Add one.](#)

Endpoints

This user has no devices.

Hardware Tokens

Add Hardware Token

This user has no hardware tokens. [Add one.](#)

Bypass Codes

Add Bypass Code

This user has no bypass codes. [Add one.](#)


WebAuthn & U2F

Add Security Key


5. Type in the user's phone number and click **Add Phone**

Dashboard > Users > duovpn > Add Phone

Add Phone

 [Learn more about Activating Duo Mobile](#)

Type Phone Tablet

Phone number  [Show extension field](#)




Optional. Example: "+52 1 222 123 4567"

Add Phone

6. Navigate to **Phones** section and click **Activate Duo Mobile**.

Phones [Add Phone](#)

You may rearrange the phones by dragging and dropping in the table. [Learn more about activating a replacement phone](#)

Alias	Device	Platform	Model	Security Warnings	
phone1		Android 10		✓ No warnings	Activate Duo Mobile 


7. Click **Generate Duo Mobile Activation Code**.

Dashboard > Activate Duo Mobile


Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application or authenticate via Duo Push.

Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this phone.

Phone 

Expiration after generation

 **Generate Duo Mobile Activation Code**

8. Select **Email** in order to receive the instruction via email, type your email address and click **Send Instructions by email**.

Dashboard > Activate Duo Mobile

Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows a mobile device to authenticate via Duo Push.

Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the r

Phone

XXXXXXXXXX

Send links via

SMS

Email



Email



9. You receive an email with the instructions, as show in the image

This is an automated email from Duo Security.

Your organization invites you to set up Duo Mobile on your phone. You will find instructions from your Duo administrator below. If you have questions, please reach out to your organization's IT or help desk team.

This email will help you add your Cisco account to Duo Mobile on this device:



Just tap this link from + [blurred] or copy and paste it into Duo Mobile manually:



If you're not reading this from + [blurred] Duo Mobile on your phone and scan this barcode:



Don't have Duo Mobile yet? Install it first:

iPhone: <https://itunes.apple.com/us/app/duo-mobile/id422663827>

Android: <https://play.google.com/store/apps/details?id=com.duosecurity.duomobile>

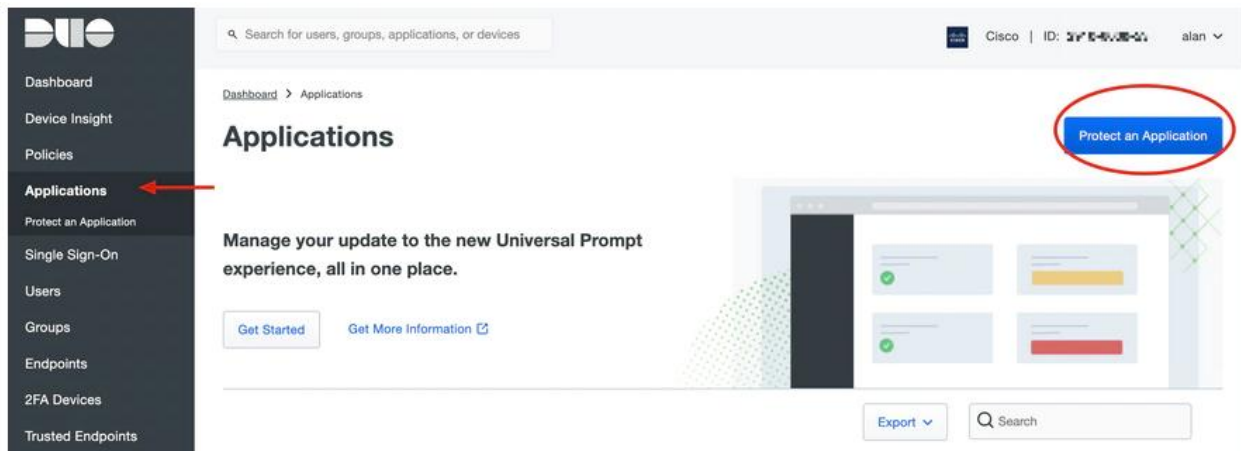
10. Open the Duo Mobile App from your mobile device and click **Add** then select **Use QR code** and scan the code from the instructions email.

11. New user is added to your Duo Mobile App.

Duo Authentication Proxy Configuration

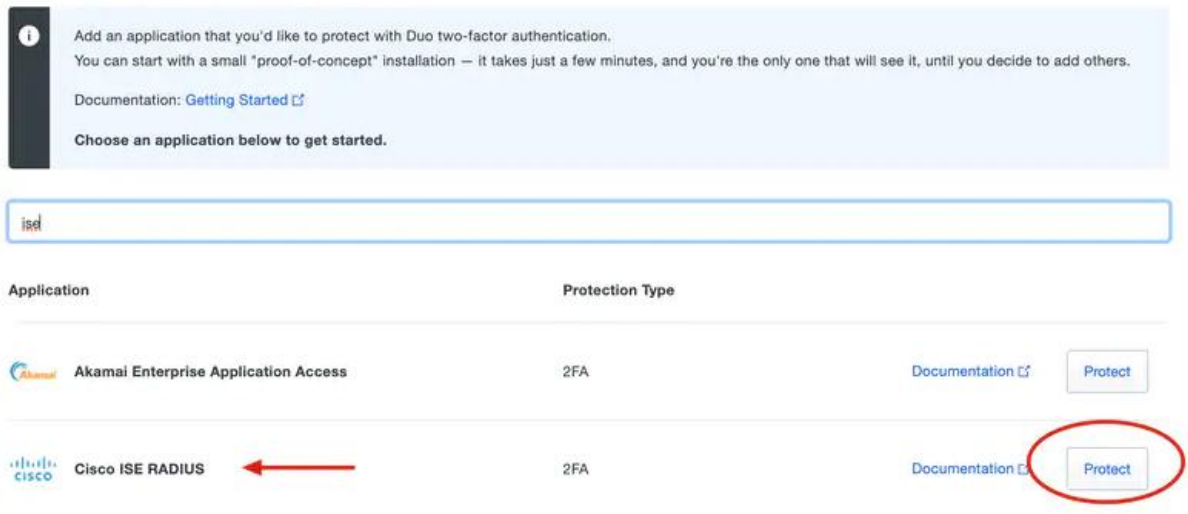
1. Download and Install Duo Auth Proxy manager from <https://duo.com/docs/authproxy-reference>.

2. On the Duo Admin Panel navigate to **Applications** and click **Protect an Application**.



3. On the search bar, look for Cisco ISE Radius.

Protect an Application



4. Copy the Integration key, Secret key and the API Hostname. You need this information for the Duo Authentication Proxy configuration.

Below is sample configuration of authproxy.cfg

- Primary authenticator, Windows Active Directory Server is on **172.16.0.14**
- Duo Authentication Proxy manager is on Windows Server **172.16.0.40**
- WTI Device is on **172.16.0.44**
- Cisco ISE is on **172.16.0.49**

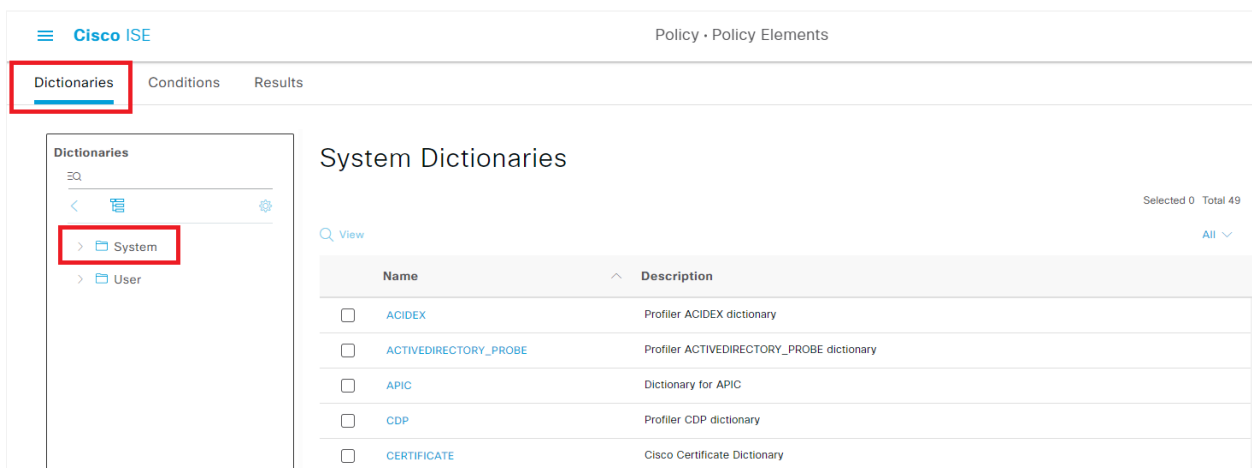
```
[ad_client]
host=172.16.0.14
service_account_username=duouser
service_account_password=duosecret
search_dn=DC=wti-lab,DC=com
security_group_dn=CN=DUO,OU=IT Department,DC=wti-lab,DC=com
```

```
[radius_server_auto]
ikey=XXXXXXXXXXXXXXXXXXXX
skey=YYYYYYYYYYYYYYYYYYY
api_host=api-123456789.duosecurity.com
radius_ip_1=172.16.0.49
radius_secret_1=test123
client=ad_client
port=1812
```

Cisco ISE Configurations

Step 1: Create vendor-specific attribute

1. Navigate to **Policy > Policy Element > Dictionaries > System > Radius > Radius Vendors > Add**



The screenshot shows the Cisco ISE interface for Policy Elements. The 'Dictionaries' tab is selected and highlighted with a red box. In the left sidebar, the 'System' folder is also highlighted with a red box. The main content area displays 'System Dictionaries' with a table of existing dictionaries. The table has columns for 'Name' and 'Description'. The following table represents the data shown in the screenshot:

Name	Description
<input type="checkbox"/> ACIDEX	Profiler ACIDEX dictionary
<input type="checkbox"/> ACTIVE DIRECTORY_PROBE	Profiler ACTIVE DIRECTORY_PROBE dictionary
<input type="checkbox"/> APIC	Dictionary for APIC
<input type="checkbox"/> CDP	Profiler CDP dictionary
<input type="checkbox"/> CERTIFICATE	Cisco Certificate Dictionary

Dictionaries

EQ

< [List Icon] [Settings Icon]

- > Posture
- > PROFILER
- ▼ RADIUS
- > IETF
- ▼ RADIUS Vendors
- > Airespace
- > Alcatel-Lucent
- > Aruba
- > Brocade
- > Cisco
- > Cisco-BBSM
- > Cisco-VPN3000
- > H3C
- > HP
- > Juniper
- > Microsoft

RADIUS Vendors

[Edit](#)
[+ Add](#)
[Delete](#)
[Import](#)
[Export](#)

<input type="checkbox"/>	Name	Vendor ID	Description
<input type="checkbox"/>	Airespace	14179	Dictionary for Vendor Airespace
<input type="checkbox"/>	Alcatel-Lucent	800	Dictionary for Vendor Alcatel-Lucent
<input type="checkbox"/>	Aruba	14823	Dictionary for Vendor Aruba
<input type="checkbox"/>	Brocade	1588	Dictionary for Vendor Brocade
<input type="checkbox"/>	Cisco	9	Dictionary for Vendor Cisco
<input type="checkbox"/>	Cisco-BBSM	5263	Dictionary for Vendor Cisco-BBSM
<input type="checkbox"/>	Cisco-VPN3000	3076	Dictionary for Vendor Cisco-VPN3000
<input type="checkbox"/>	H3C	25506	Dictionary for Vendor H3C
<input type="checkbox"/>	HP	11	Dictionary for Vendor HP
<input type="checkbox"/>	Juniper	2636	Dictionary for Vendor Juniper
<input type="checkbox"/>	Microsoft	311	Dictionary for Vendor Microsoft
<input type="checkbox"/>	Motorola-Symbol	388	Dictionary for Vendor Motorola-Symbol
<input type="checkbox"/>	Ruckus	25053	Dictionary for Vendor Ruckus
<input type="checkbox"/>	WISPr	14122	Dictionary for Vendor WISPr
<input type="checkbox"/>	WTI	24496	Dictionary for Vendor WTI

2. The name and the Vendor IDs are to be entered and saved.

Dictionary Name: **WTI**

Vendor ID: **24496**

Cisco ISE Policy · Policy Elements

Dictionaries Conditions Results

Dictionaries

EQ

< [List Icon] [Settings Icon]

- > PassiveID
- > Posture
- > PROFILER
- ▼ RADIUS
- > IETF
- > RADIUS Vendors
- > Session
- > SNMP
- > SPHUB
- > SXP

RADIUS Vendors List > New RADIUS Vendor

* Dictionary Name

Description

* Vendor ID

Vendor Attribute Type Field Length

Vendor Attribute Size Field Length

[Dictionaries](#) [Conditions](#) [Results](#)

Dictionaries

EQ

<

- > NMAPExtension
- > Normalised Radius
- > PassiveID
- > Posture
- > PROFILER
- ▼ Radius
 - > IETF
 - > RADIUS Vendors

Dictionaries > ... > RADIUS Vendors > **WTI**

Dictionary **Dictionary Attributes**

Dictionary Attributes

+ Add Edit Delete

<input type="checkbox"/>	Name	Number	Type	Direction	Description	Predefi...
<input type="checkbox"/>	WTI-Super	41	INT	BOTH		NO

4. Click Add and fill out the Attribute Name, Data Type, Direction and ID and Add allow values for access level.

Attribute Name: **WTI-Super**

Data Type: **INT**

Direction: **BOTH**

ID: **41**

Add allow Values for access level

Name: **Administrator**

Value: **3**

Name: **User**

Value: **1**

[Dictionaries](#) [Conditions](#) [Results](#)

Dictionaries

EQ

<

- > NMAPExtension
- > Normalised Radius
- > PassiveID
- > Posture
- > PROFILER
- ▼ Radius
 - > IETF
 - ▼ RADIUS Vendors
 - > Airespace
 - > Alcatel-Lucent
 - > Aruba
 - > Brocade
 - > Cisco
 - > Cisco-BBSM
 - > Cisco-VPN3000
 - > H3C

Dictionaries > ... > WTI > **WTI-Super**

** Attribute Name*

Description

* Data Type ▼

* Direction ▼

* ID (0-255)

Allow Tagging

Allow multiple instances of this attribute in a profile

Allowed Values

+ Add Delete

<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	Administrator	3
<input type="checkbox"/>	User	1

Selected 0 Total 2

Save
Reset

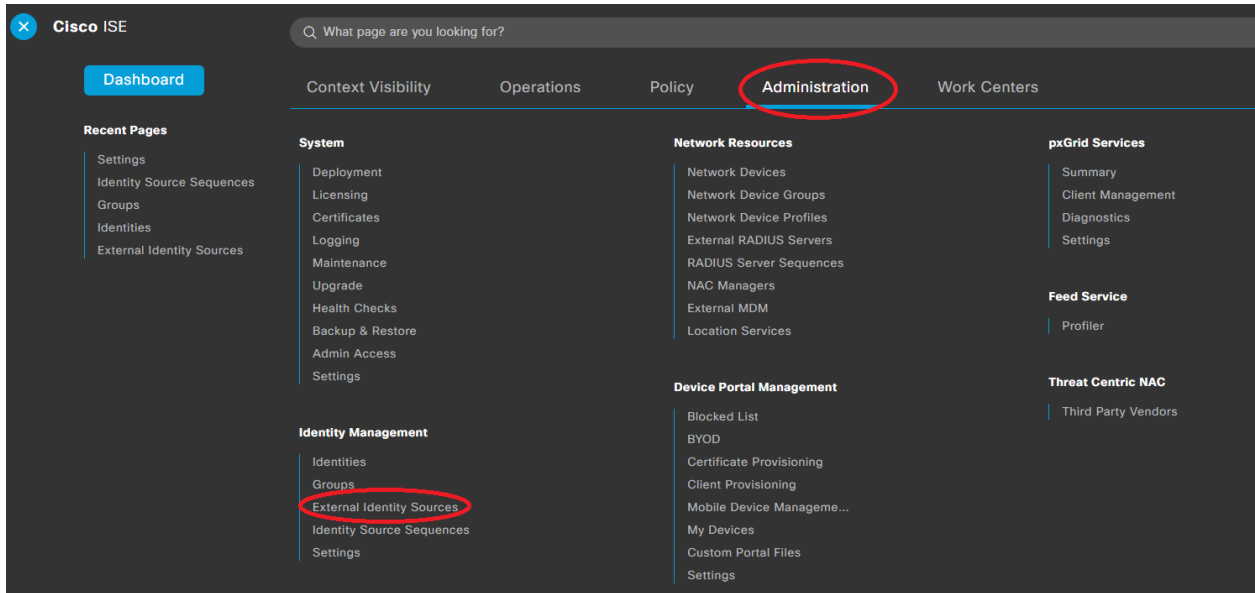
5. Save the attribute.

6. Add other Attributes on the same page if there are multiple Attributes to be added to the same Dictionary.

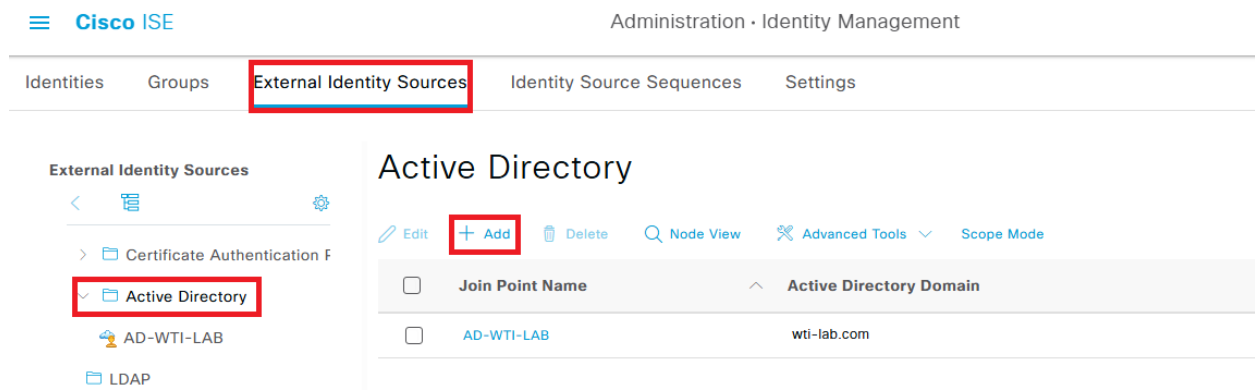
WTI RADIUS Dictionary <https://ftp.wti.com/InfoCenter/rsa/dictionary/dictionary.wti>

Step 2: Connect Active Directory joint point in ISE

1. Navigate to **Administration** then click **Identity Management** and click **External Identity Sources**.



2. On **External Identity Sources** tab, Navigate to Active Directory and click **Add**



3. Under Connection section. Fill in the all requirement and click submit.

Cisco ISE Administration · Identity Management

Identities Groups **External Identity Sources** Identity Source Sequences Settings

External Identity Sources

- Certificate Authentication F
- Active Directory
 - AD-WTI-LAB
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID

Connection Allowed Domains PassivelD Groups Attributes Advanced Settings

Join Point Name AD-WTI-LAB

Active Directory Domain wti-lab.com

+ Join + Leave Test User Diagnostic Tool Refresh Table

<input type="checkbox"/>	ISE Node	ISE Node R...	Status	Domain Controller	Site
<input type="checkbox"/>	CiscolSE.wti-lab.com	STANDALONE	Operational	DCWin2022.wti-lab.com	Default-First-Site-Name

4. Navigate to Groups tab and click Add > Select Group from Directory.

Cisco ISE Administration · Identity Management

Identities Groups **External Identity Sources** Identity Source Sequences Settings

External Identity Sources

- Certificate Authentication F
- Active Directory
 - AD-WTI-LAB
- LDAP

Connection Allowed Domains PassivelD **Groups** Attributes Advanced Settings

Edit + Add Delete Group Update SID Values

<input type="checkbox"/>	Name	SID
<input type="checkbox"/>	wti-lab.com/IT Department/DUO	S-1-5-21-2346001846-3831695603-2264274261-2642

5. Configuration for RADIUS communication between ISE and DUO. Navigate to Work Center > Device Administration > Ext Id Sources

Cisco ISE

Q: What page are you looking for?

Dashboard Context Visibility Operations Policy Administration **Work Centers**

Recent Pages

- Ext Id Sources
- External Identity Sources
- Identity Source Sequences
- Policy Sets
- Device Admin Policy Sets
- Settings

Network Access

- Overview
- Identities
- Id Groups
- Ext Id Sources
- Network Resources
- Policy Elements
- Policy Sets
- Troubleshoot
- Reports

TrustSec

- Overview
- Components
- TrustSec Policy
- Policy Sets
- SXP
- ACI
- Troubleshoot
- Reports
- Settings

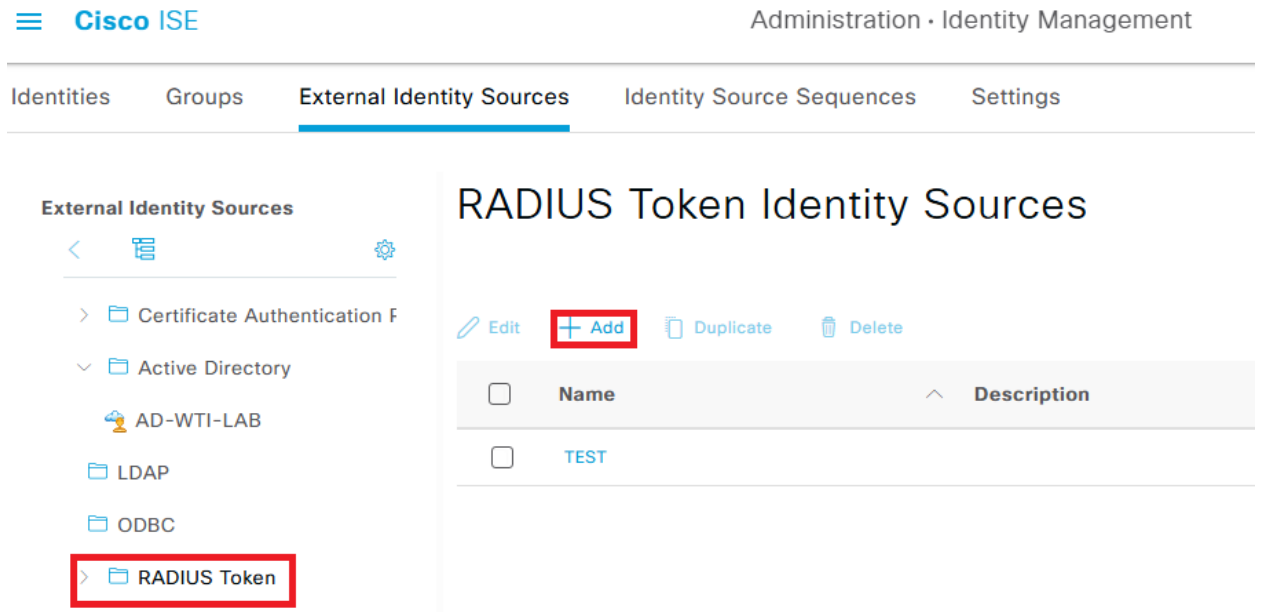
Profiler

- Overview
- Ext Id Sources
- Network Devices
- Endpoint Classification
- Node Config
- Feeds
- Manual Scans
- Policy Elements
- Profiling Policies

Device Administration

- Overview
- Identities
- User Identity Groups
- Ext Id Sources**
- Network Resources
- Policy Elements
- Device Admin Policy Sets
- Reports
- Settings

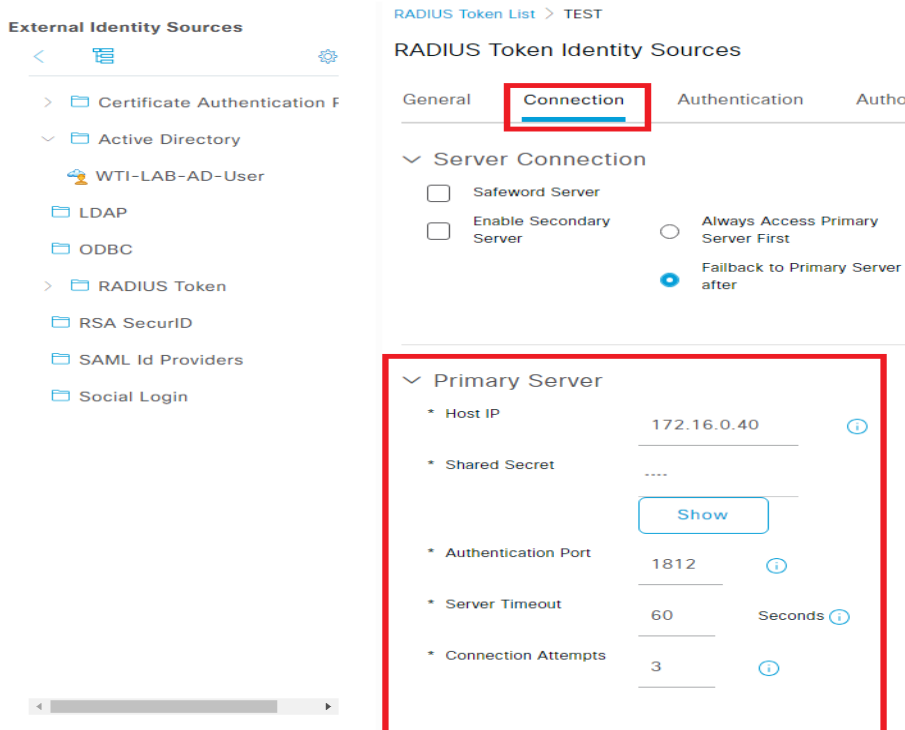
6. On RADIUS Token click **Add**.



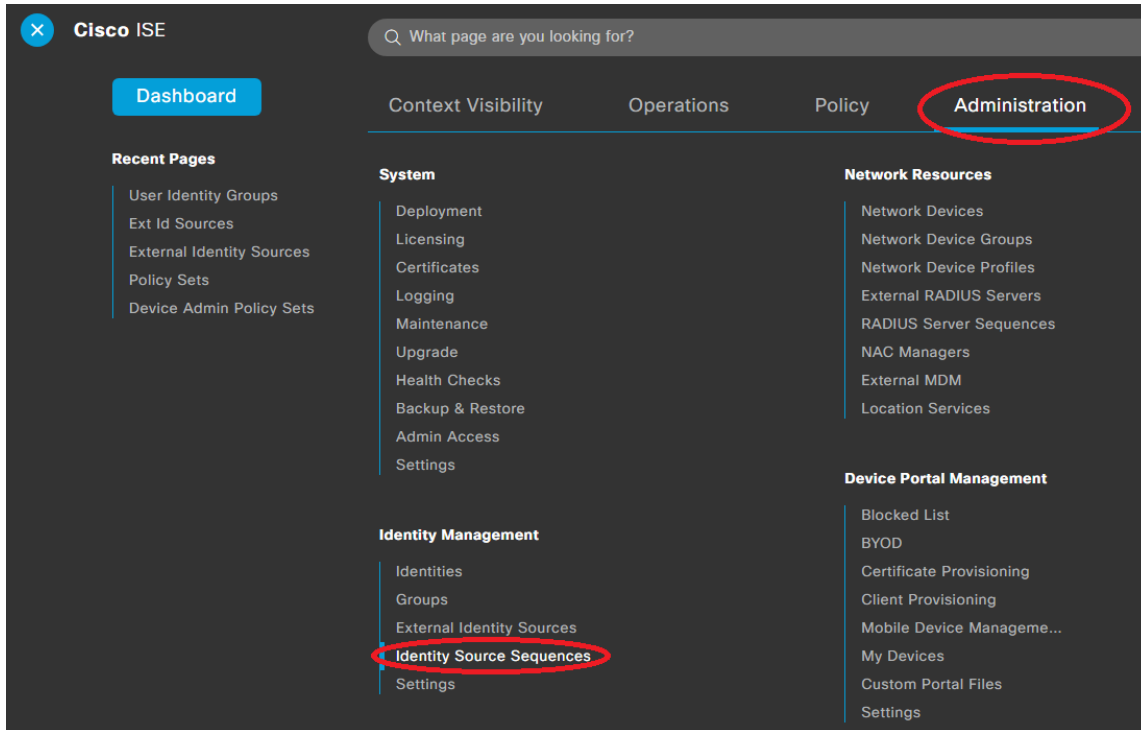
7. Starting from the left to right, configure the settings within each tab menu item as follow.

a. In General tab, configure the name for the configuration.

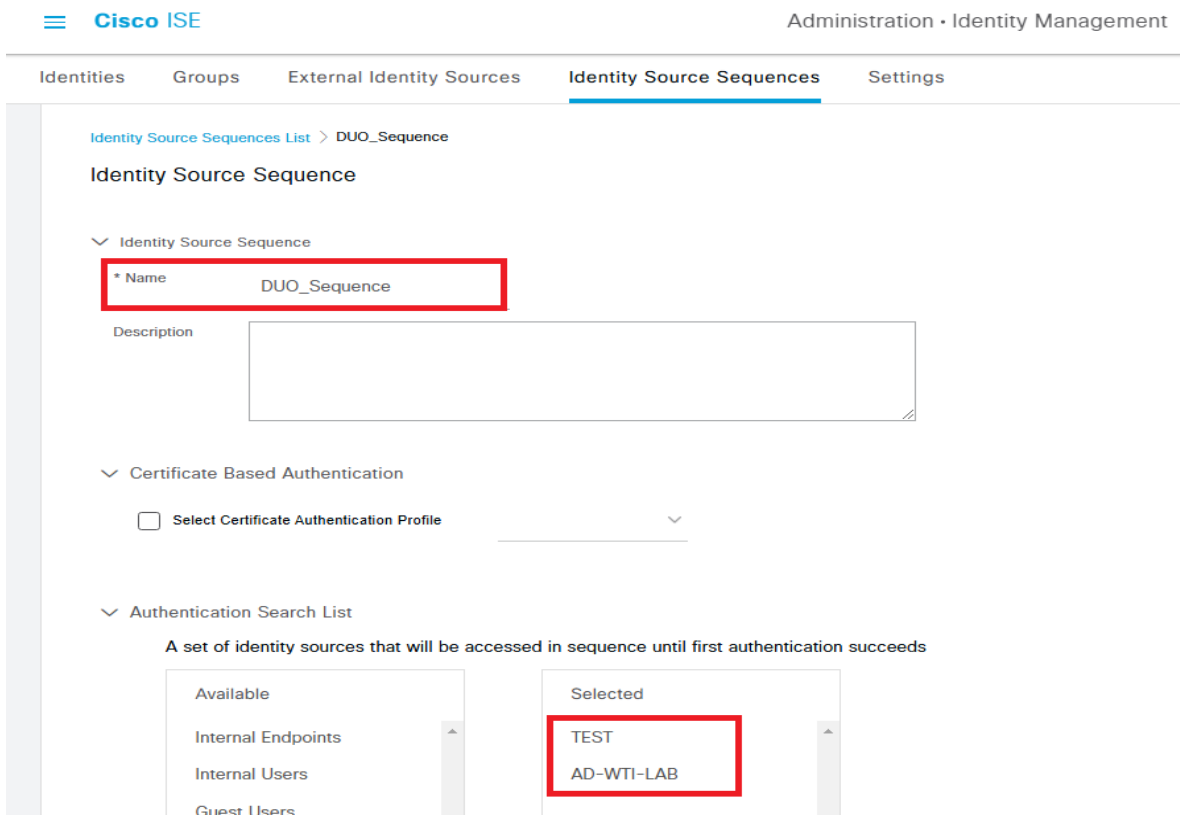
b. In Connection tab, configure the primary server details. (Primary Server is DUO Proxy Authentication Server)



8. Create Identity Source sequences. Navigate to **Administration > Identity management > Identity Sources Sequence**

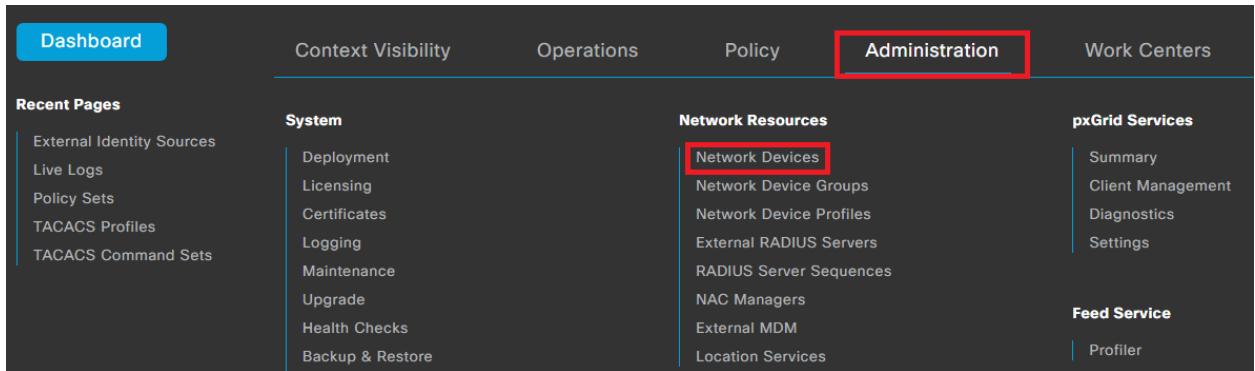


9. In Identity Sources Sequence click **Add** name identity source sequence and select authentication available search list and click Save.

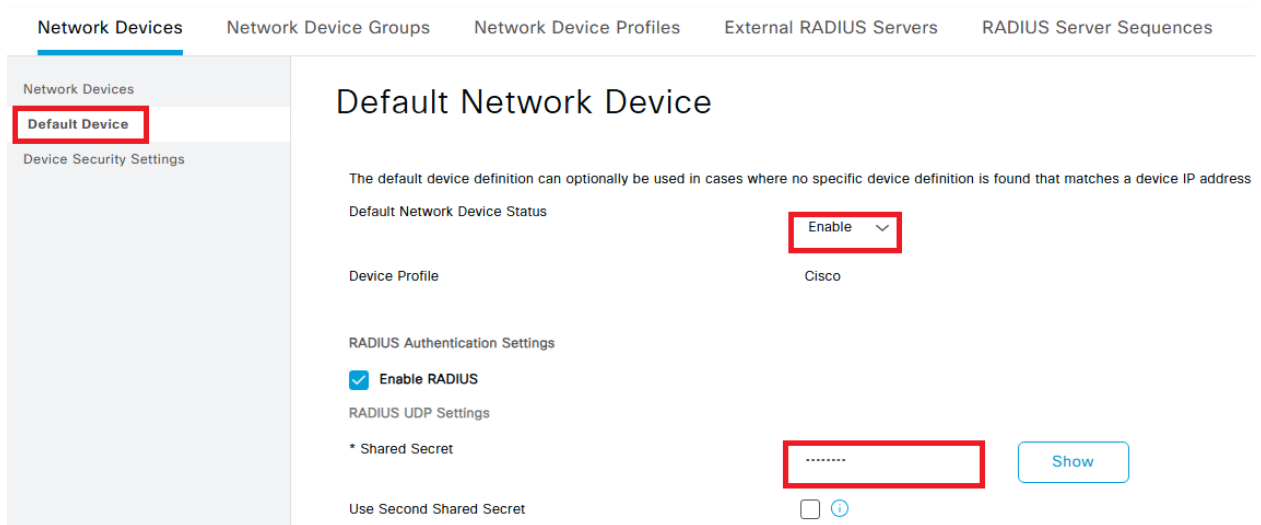


Step 3: Create Network Device

1. Navigate to **Administrator > Network Resource > Network Device**

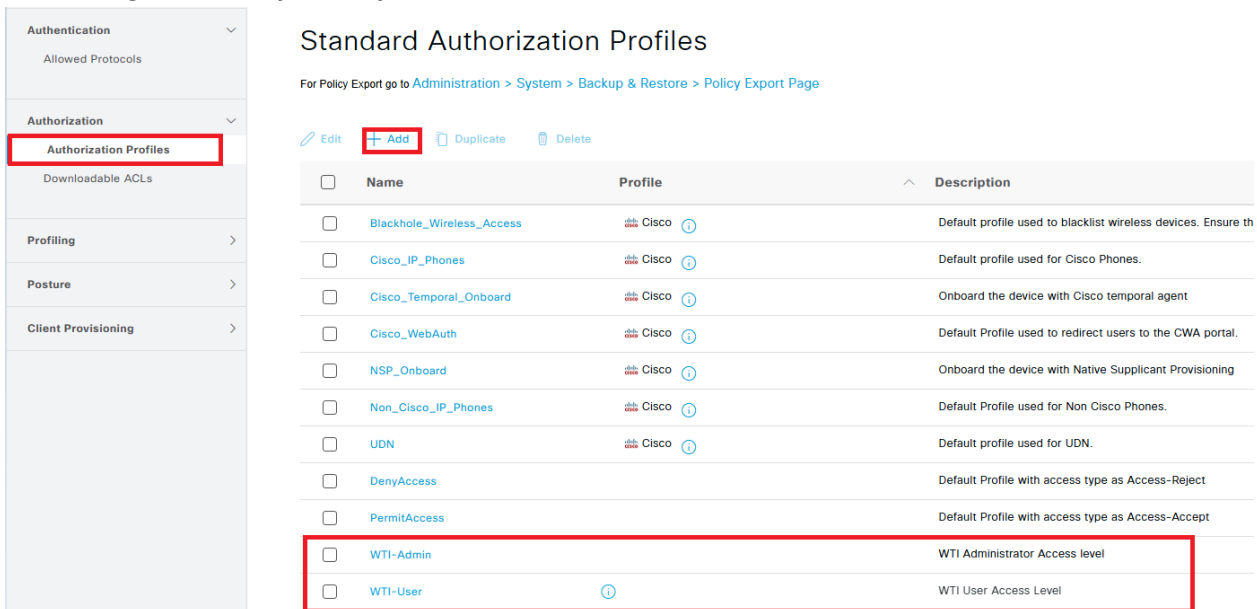


2. Enable Radius and define shared secret in Device Default



Step 4: Create Radius Authorization Profile

1. Navigate to **Policy > Policy Elements > Results > Authorization Profiles > Add**



2. Create two Authorization Profile. One for WTI_Admin (Administrator access level) and another for WTI_User (User access level).

The screenshot shows the configuration page for an Authorization Profile named "WTI-Admin". The page is divided into several sections:

- Authentication:** Allowed Protocols
- Authorization:** Authorization Profiles (selected), Downloadable ACLs
- Profiling:** >
- Posture:** >
- Client Provisioning:** >

The main configuration area includes:

- Name:** WTI-Admin
- Description:** WTI Administrator Access level
- Access Type:** ACCESS_ACCEPT
- Network Device Profile:** Any
- Service Template:**
- Track Movement:** ⓘ
- Agentless Posture:** ⓘ
- Passive Identity Tracking:** ⓘ

Under **Common Tasks**:

- Web Redirection (CWA, MDM, NSP, CPP) ⓘ
- Unique Identifier ⓘ

Under **Advanced Attributes Settings**, a rule is defined: **WTI:WTI-Super = Administrator**. This rule is highlighted with a red box.

For WTI_Admin

In advanced Attribute Settings

Advanced Attributes Settings

A close-up of the rule configuration in the Advanced Attributes Settings section. The rule is: **WTI:WTI-Super = Administrator**. The rule is highlighted with a red box.

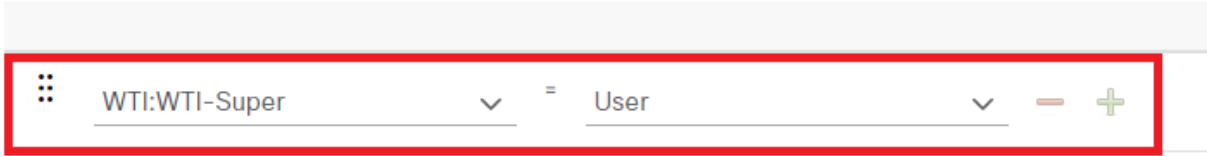
Attributes Details

A close-up of the Attributes Details section. The attributes are: **Access Type = ACCESS_ACCEPT** and **WTI-Super = 3**. This section is highlighted with a red box.

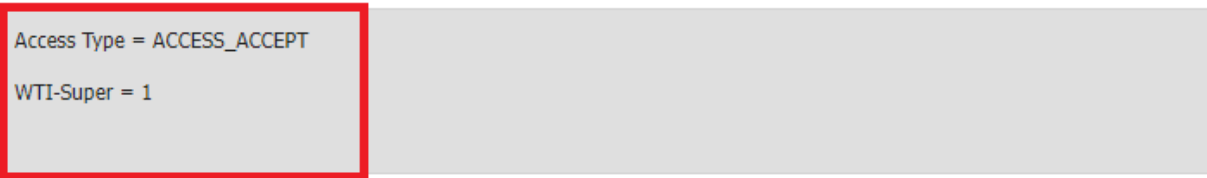
For WTI_User

In Advance Attribute Settings

Advanced Attributes Settings

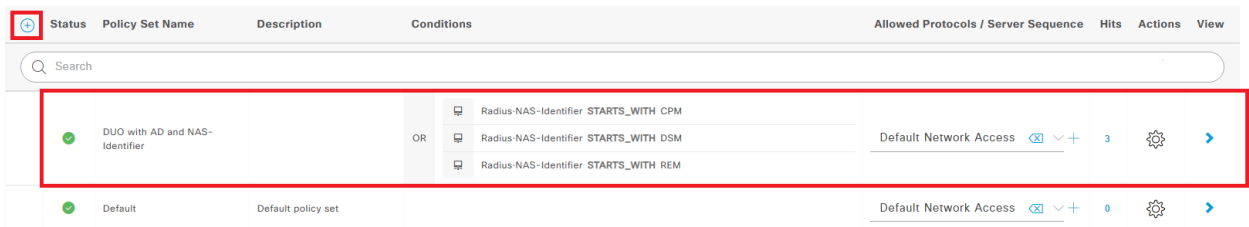


Attributes Details



Step 5: Create Policy with NAS-Identifier

1. Navigate to **Policy > Policy Sets > click (+) to add new policy set.**



Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	DUO with AD and NAS-Identifier		OR Radius-NAS-Identifier STARTS_WITH CPM Radius-NAS-Identifier STARTS_WITH DSM Radius-NAS-Identifier STARTS_WITH REM	Default Network Access	3		
	Default	Default policy set		Default Network Access	0		

Policy Set Name: **DUO with AD and NAS-Identifier**

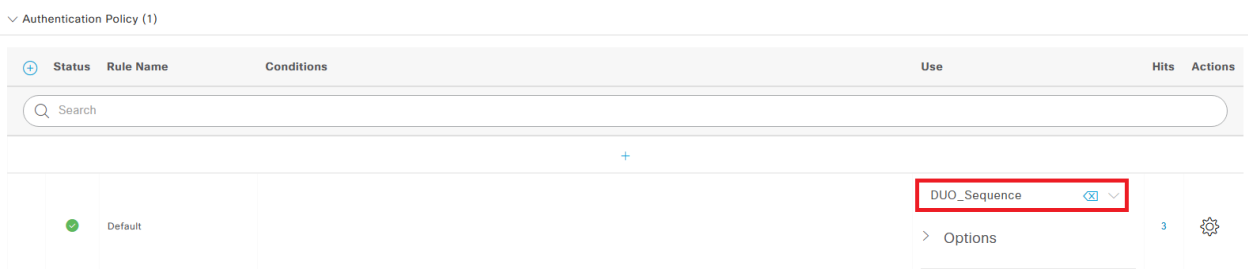
Condition: **Radius-NAS-Identifier START_WITH CPM (DSM or REM)**

Allowed Protocols: **Default Network Access**

2. Authentication Policy

Rule Name: Default

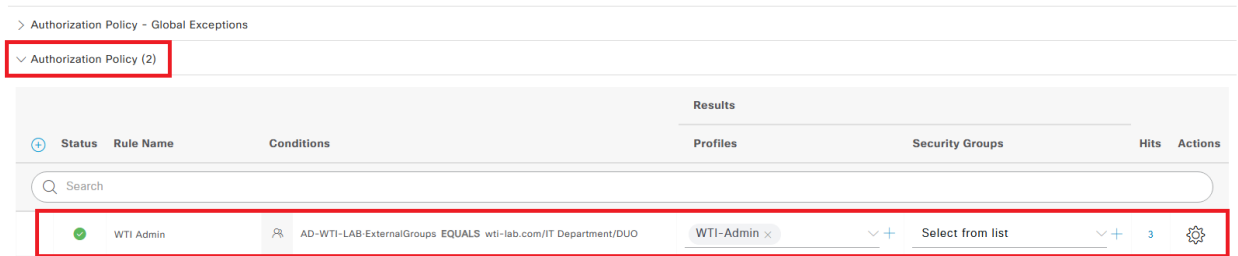
Use: **DUO_Sequence**



Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
	Default		DUO_Sequence	3	

3. Authorization Policy – create two authorization policy, one for WTI_Admin and another for WTI_User.

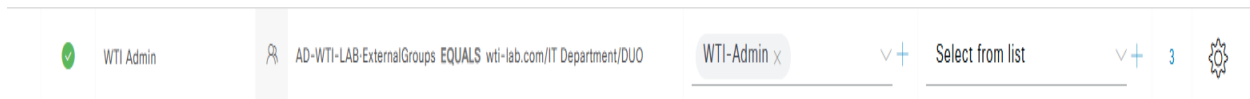


For WTI_Admin

Rule Name: **WTI-Admin**

Condition: **AD-WTI-LAB-ExternalGroup EQUALS wti-lab.com/IT Department/DUO**

Profile: **WTI_Admin**

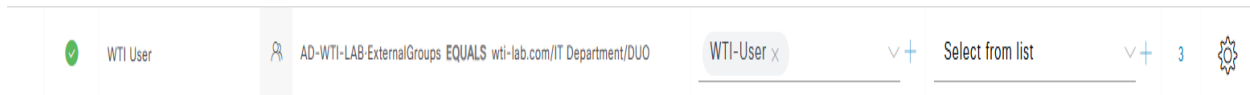


For WTI_User

Rule Name: **WTI-User**

Condition: **AD-WTI-LAB-ExternalGroup EQUALS wti-lab.com/IT Department/DUO**

Profile: **WTI_User**



WTI Radius Setting

1. Go to /N option 29 for Radius
2. RADIUS Setting

```
RADIUS: [Shared]
1. Enable: On
2. Primary Host/Address: 172.16.0.49
3. Primary Secret Word: <defined>
4. Secondary Host/Address: <undefined>
5. Secondary Secret Word: <undefined>
6. Fallback Timer: 30 Sec
7. Fallback Local: On <All failures>
8. Retries: 3
9. Authentication Port: 1812
10. Accounting Port: 1813
11. Default User Access: Off
12. OneTime Auth: On
13. OneTime Auth Timer: 15
14. OneTime Auth Type: Cookies
15. Session Module Type: Disable
16. Require Message Authentic: Off
17. Debug: On
18. Ping Test
```